WC Docket No. 05-271
Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matters of	)	
	)	
Appropriate Framework for Broadband Access to the Internet over Wireline Facilities	)	CC Docket No. 02-33
	)	
Universal Service Obligations of Broadband Providers	)	CC Docket No. 01-337
Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services	)	
	)	
Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review – Review of Computer III and ONA Safeguards and Requirements	)	CC Docket Nos. 95-20, 98-10
	)	
Conditional Petition of the Verizon Telephone Companies for Forbearance Under 47 U.S.C. § 160(c) with Regard to Broadband Services Provided Via Fiber to the Premises; Petition of the Verizon Telephone Companies for Declaratory Ruling or, Alternatively, for Interim Waiver with Regard to Broadband Services Provided Via Fiber to the Premises	)	WC Docket No. 04-242
	)	WC Docket No. 05-271
Consumer Protection in the Broadband Era		

INTRODUCTION

The Federal Communications Commission (FCC) has sought comment on various issues regarding the development of a consumer protection framework for the "broadband era." With expanding broadband technology, we are seeing the

depth and diversity of services the internet provides. However, with this expansion comes a need to ensure that end user consumers are protected. While the expansion of broadband affords a great many positive opportunities, it also has the side effect of creating nefarious opportunities.

This comment letter will cover three of the specified areas for comment in the Notice for Proposed Rule Making (NPRM); Consumer Proprietary Network Information concerns, Slamming, and Network Outage Reporting.

JURISDICITON

According to the NPRM, the FCC asserts that its jurisdiction to regulate and mandate a broadband framework stems from its Title 1 ancillary jurisdiction. This ancillary jurisdiction designates to the FCC the authority to regulate all "services incidental to" wire communications[1]. While this jurisdictional component is likely to be sufficient (as the Commission points out), it should be taken into consideration that the recent DC Circuit case, *Am. Library Ass'n v. FCC*, 406 F.3d 689 (DC Cir. 2005) has placed a possible limit to this jurisdiction. *Am Library Ass'n* could possibly end the FCC's jurisdiction at the point an initial transmission or communication terminates. It is unclear how this possible limitation would apply to the broadband context – however, because it appears that previously unaccounted for limits to the FCC's ancillary jurisdiction may exist, the Commission should explore other jurisdiction authority for this NPRM. This will be particularly important when dealing with any regulations that could implicate an end-user piece

[1] 47 USCS §153 (52).

of hardware, *after* an initial transmission termintes.

CONSUMER PROPRIETARY NETWORK INFORMATION

One of the issues the Commission seeks comment on is that of consumer proprietary network information (CPNI) security. In the broadband era, information has become an asset. This is evidenced by such industry practices as "email address harvesting"[2] and targeted online advertising like "AdSense."[3] These practices have placed an incredible value on an individual's online conduct. In particular, online advertisers are increasingly interested in how their customers came to their site, and what else they might have been looking at online[4]. These privacy issues have also arisen in the digital era with respect to cell phone records. Some reports have been made detailing the ease with which one can obtain any person's cell phone records for a fee.[5] At the end, all of this information is worth a great deal of money to interested parties. Marketing interests could conceivably obtain very specific details about the success and even potential success of future or current ventures.

This issue raises the question of whether or not an individual can consider their online browsing choices personal information, and in turn, that they (the end-user) has some innate right to this information. In the criminal context, generally, "what a person knowingly exposes to the public, even in his own home or office, is

---

[2] http://en.wikipedia.org/wiki/Email_address_harvesting
[3] http://en.wikipedia.org/wiki/AdSense
[4] see; http://www.google.com/analytics/
[5] see; "Carriers struggle to protect privacy while helping law enforcement" RCR Wireless news, 1/16/2006; available at: http://www.rcrnews.com/lockland.cms?articleId=49808

not a subject of Fourth Amendment protection."[6] Hence, one could state generally, that we do not have any kind of privacy right to that information which we knowingly put out to the public.[7]

This begs the question however, as to what level of privacy an individual sitting in their home, using their personal computer has over the "information" they send out over the internet. To the lay user, the mere click on an online advertisement may not be seen as any kind of assertion. Most lay users would consider this a totally innocuous action. However, things like "identity theft"[8], phishing[9] and pharming[10] scams are on the rise[11] and are slowing bringing online security and privacy issues to the forefront of the digital era. The idea that what the end-user does online on his or her home computer is not necessarily private is slowing making its way into the modern mentality.

There are options available to the more "web-savvy" internet users to protect their identity while online. Most notably is the option of browsing the internet via a web-based internet browsing proxy.[12] Many free web-based internet browsing proxy sites exist online[13]. These are often very easy to use, however, can sometimes slow down web browsing considerably. Another concern exists in that the proxy site itself may be able to collect the very same information the end-user is seeking to

---

[6] *Katz v. United States*, 389 U.S. 347 at 351 (1967).
[7] While it is true that the 4th Amendment only provides these protections in the scope of criminal prosecutions, theoretically, it still provides us with a decent idea of what privacy rights *could* be considered constitutionally valid.
[8] http://en.wikipedia.org/wiki/Identity_theft
[9] http://en.wikipedia.org/wiki/Phishing
[10] http://en.wikipedia.org/wiki/Pharming
[11] see; http://www.cnn.com/2005/TECH/internet/09/26/identity.hacker/index.html
[12] see for example; http://www.the-cloak.com/anonymous-surfing-faq.html
[13] see for example; http://anonymouse.org/anonwww.html

keep hidden from his/ Internet Service Provider.

Overall – as there appears to be some evidence of an expectation of privacy for information submitted online, the Commission should consider how important an end-users' privacy is. Common sense would dictate that so long as the end-user's actual identity is concealed, that many of the privacy concerns would be moot. However, the commoditization of semi-personal information, like a consumers' service plan and patterns of use, raises an in intriguing issue. The issue being, who has a right to this information? It would appear that so long as the end-users' name is concealed, any privacy concern would be eliminated. Hence, there does not seem as if an end user can assert any claim or right over this information.

As such, it would make sense for the Commission to mandate that service providers respect end-user privacy and never distribute any identity revealing information. Also, in order to avert any possible claims, service providers could be required to provide an "opt-out" option for end-users, so that those users who do not want their internet activity distributed can make it known.

This does not however reach the issue of whether or not this information can be considered the right, or "property" of the end-user. In other words, because this information is considered so valuable to companies willing to pay for it – should the end-user be the one getting paid? As it is unclear whether or not the end-user can assert any definitive right over this information, it would not appear that ISPs need to be worried about it. However, to avert any potential future issues, ISPs could, and possibly should be encouraged to pass on the profits obtained from selling CPNI

to end-users in the form of a price reduction. For instance, the ISP could provide the option of "opting out" for an end user from having their CPNI distributed. However, to entice end-users to allow their non-identity revealing information to be distributed, if they "opt-in" they could be rewarded with a discount on their normal ISP service charges.

SLAMMING

Slamming is the practice of switching an individual's telephone service without their knowledge, and often without their true consent.[14] In the broadband era, as noted by the Commission, slamming would be a problem due to the required terminating end hardware. This hardware is most often either a "cable modem"[15] or a "DSL modem"[16].

In particular, slamming may be seen as a moot issue for individual end users who have broadband access via a cable modem. This is mainly because most markets have only one sole cable broadband provider, due to the fact that cable is a natural monopoly. There have been, however, some alleged instances of slamming already in the cable arena[17]. Cable based slamming will likely be a very limited problem, as today, only 5 cable providers account for nearly 75% of all cable network access.[18] Only in the increasingly limited areas where some overlap exists, or a major provider has not taken over, will slamming be an issue with cable. As such,

---

[14] http://en.wikipedia.org/wiki/Telephone_Slamming
[15] http://en.wikipedia.org/wiki/Cable_Modem
[16] http://en.wikipedia.org/wiki/DSL_modem; DSL = Direct Subscriber Line.
[17] http://www.mediasf.org/index.php/news/206
[18] http://en.wikipedia.org/wiki/List_of_cable_companies#United_States

the mere market forces of a natural monopoly like cable will likely make slamming a moot issue in this arena.

In the area of DSL, there may be more of an issue with regard to slamming. Essentially, any service provider can provide a connection to the internet via telephone lines using DSL technology.[19] Essentially, this could lead to a similar problem with slamming as was seen with the long-distance carrier slamming that spawned the Commissions prior anti-slamming regulations[20].

There is a significant extra technological step that a service provider must overcome before slamming an end-user. This extra step is that of potential hardware compatibility issues with DSL modems. Currently, not all DSL modems are compatible with all service providers[21]. This may, as often is with technological hurdles, be only a temporary problem. As technology develops, the interoperability of DSL modems is likely to increase as manufactures will likely aim to provide DSL modems that are compatible with any service provider.

Overall, it appears unclear how much on an impact slamming may have on broadband internet. Most likely, it would seem to have the potential to affect DSL service. As it seems to be a possibility for DSL, and has apparently been occurring with cable service, the Commission should impose anti-slamming requirements on broadband service providers.

---

[19] http://electronics.howstuffworks.com/dsl.htm; http://en.wikipedia.org/wiki/Digital_Subscriber_Line
[20] 47 U.S.C. §258(a)
[21] http://www.dsldepot.com/dslprovider.asp

NETWORK OUTAGE REPORTING

Current regulations on network outage reporting covers; cable communications providers, satellite communications providers, signaling system 7, wireless service providers, and wireline communications providers[22]. Network outage reporting is most critical for broadband providers in the area of Voice over Internet Protocol (VoIP). VoIP is a growing trend in which customers can use their broadband connections to make and receive telephone calls.[23] Network outage reporting is of key significance for VoIP most notably because of 911 emergency access.

It would appear that the current regulations would require cable based phone systems to report network outages. Hence, cable based VoIP will likely not be at issue. There are also many individuals who use VoIP over a DSL broadband connection. In this case, while the wireline service of the physical phone line involved may be required to report a network outage, the actual service provider does not appear to be covered by the current regulations. Emergency 911 systems are a very important public safety concern. For individuals who do not have a plain old telephone system (POTS) connection, and who use VoIP exclusively, VoIP could possibly be their only way to contact an emergency 911 dispatch center. Hence, for all the reason for which a wireline POTS provider must report a network outage, a DSL service provider through whom a subscriber may be using VoIP should be

[22] 47 CFR 4.3 (a)-(h)
[23] http://en.wikipedia.org/wiki/Voice-over-IP

required to report network outages.

There are other concerns for broadband network outage reporting. In the broadband era, many businesses rely on their broadband connections. Network outages can have a major detrimental economic impact on a business reliant on its broadband connection. Any outages also provide a major hassle and annoyance for many other professionals and lay users. While these concerns should be considered, they are not as pressing of a concern as access to emergency 911 services. However, they do add weight to the argument that network outage reporting requirements be extended to broadband service providers across the board.

CONCLUSION

In Conclusion, the FCC should first more closely examine its jurisdiction to implement all of the aforementioned proposed rules, especially with respect to regulations that would affect end-user hardware specifications.

In an effort to respect individual privacy, regulations with respect to CPNI should at the very least completely conceal an end user's identity.

As it is unclear how pervasive a problem slamming may be for broadband internet connections, the FCC should proceed with further inquiries to service providers to determine whether this problem is currently an issue. As there does appear to be potential for this to develop, much as it did with telephone long distance carriers before, regulation may be necessary.

Emergency service dispatching is a crucial public service. As more and more

people are shifting to using VoIP services, the need for a steady broadband connection is growing. As such, Network Outage Reporting should be mandated for broadband providers that carry VoIP signals. This will logically affect all broadband providers.

Respectfully Submitted,

N. Nedim Halicioglu